

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

November 07, 2003

**THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM
THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK
OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT
APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A
FILING DATE UNDER 35 USC 111.**

APPLICATION NUMBER: 60/430,206

FILING DATE: December 02, 2002



**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**

P. R. Grant

**P. R. GRANT
Certifying Officer**

12/02/02
3670 U.S. PRO

12-03-02

Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. EL 843729853US

INVENTOR(S)					
Given Name (first and middle (if any))		Family Name or Surname		Residence (City and either State or Foreign Country)	
Thomas		POHLEY		Erlangen, Germany	
<input type="checkbox"/> Additional inventors are being named on the _____ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (500 characters max)					
"Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen"					
Direct all correspondence to: CORRESPONDENCE ADDRESS					
<input checked="" type="checkbox"/> Customer Number		26574		Place Customer Number Bar Code Label here	
OR Type Customer Number here					
<input type="checkbox"/> Firm or Individual Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/> Specification		Number of Pages		18	
<input checked="" type="checkbox"/> Drawing(s)		Number of Sheets		2	
<input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76		<input type="checkbox"/> CD(s), Number			
		<input type="checkbox"/> Other (specify)			
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT					
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.				FILING FEE AMOUNT (\$)	
<input type="checkbox"/> A check or money order is enclosed to cover the filing fees				160.00	
<input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:		501519		160.00	
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
<input checked="" type="checkbox"/> No					
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are _____					

Respectfully submitted,

SIGNATURE

Steven H. Noll

Date

12-2-02

TYPED or PRINTED NAME

Steven H. Noll

TELEPHONE

312-258-5790

REGISTRATION NO.
(if appropriate)

28,982

Docket Number:

P02,0630

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

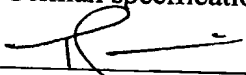
This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" Mailing Label Number **EL 843729853US**
Date of Deposit: December 2, 2002

I hereby certify that the following is being deposited with the United States Postal
"Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above
and is addressed to Hon. Assistant Commissioner of Patents, Washington DC 20231.

Provisional Patent Application for THOMAS POLHLEY consisting of 18 pages of
German specification, claims, 2 Sheets of drawings, Attorney Docket No. P02,0630



Signature of person
mailing application

CHI_DOCS2\565268.1

Beschreibung

1

Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen

5

Die Erfindung betrifft ein Verfahren zum schnellen Anmelden von Nutzern an Datenverarbeitungseinrichtungen.

Die Verarbeitung elektronischer Daten durch Datenverarbeitungseinrichtungen in Arbeitsumgebungen mit sensiblen Daten erfordert einen wirksamen Schutz der Daten vor unberechtigten Zugriffen. Es muss jederzeit sichergestellt sein, dass eine Einsichtnahme oder Veränderungen z.B. von elektronischen Patientenakten oder Bildern aus digitalen diagnostischen Bildgebungsverfahren ausschließlich durch berechtigte Personen erfolgen kann. Darüber hinaus müssen in medizinischen Arbeitsumgebungen sämtliche Zugriffe auf die sensiblen Daten so protokolliert werden, dass jederzeit nachvollziehbar ist, welche Personen Datenzugriffe welcher Art vorgenommen haben.

Bei herkömmlichen Datenträgern, wie etwa Patientenakten auf Papier oder diagnostischen Bildern auf Filmsystemen, ist eine Kontrolle des Datenzugriffs durch Kontrolle des Verbleibs der Datenträger ohne weiteres möglich. Dahingegen sind elektronische Daten ohne weiteres vielfach zugreifbar und statt des Verbleibs der Daten müssen Zugriffe darauf kontrolliert werden. Zu diesem Zweck müssen sich Nutzer von Datenverarbeitungseinrichtungen für sensible Daten, wie medizinischen Computer-Arbeitsplätzen, durch Eingabe von Nutzernamen und Passwörtern oder durch biometrische Identifikation, z.B. anhand des Fingerabdrucks, oder durch Chipkarten o.ä. identifizieren, um durch die Datenverarbeitungseinrichtung authentifiziert werden zu können. Im Rahmen der Authentifizierung wird die Identität des jeweiligen Nutzers zu Protokollierungszwecken festgestellt und der Daten- und Anwendungszugriff im für den jeweiligen Nutzer vorgesehenen Umfang autorisiert. Außer-

dem wird der Umfang der Zugriffsmöglichkeiten auf Hardware und Software festgelegt.

- Im klinischen Alltag arbeiten oft mehrere Personen, z.B. medizinisch-technische Assistentinnen oder Ärzte, abwechselnd an der gleichen Datenverarbeitungseinrichtung, z.B. einem Computer-Arbeitsplatz zur Befundung oder zur Erstellung diagnostischer Bilder. Um dem Anspruch rationeller und ökonomischer Arbeitsabläufe gerecht zu werden, muss der Nutzerwechsel möglichst schnell durchführbar sein. Soll mit der gleichen Datenverarbeitungseinrichtung oder den gleichen Patientendaten weitergearbeitet werden, müssen auch diese nach einem Nutzerwechsel möglichst schnell wieder verfügbar sein.
- 15 Bislang erfolgt die Authentifizierung eines Nutzers durch die Datenverarbeitungseinrichtung auf Betriebssystem-Ebene. Das sogenannte Login am Betriebssystem wird beim Systemstart durch Eingabe eines Nutzernamens und eines Passworts identifiziert, und in Abhängigkeit von der Identifikation werden
- 20 durch das Betriebssystem Zugriffsrechte für Daten, Hardware und Software zuerkannt. Diese Authentifizierung auf Ebene des Betriebssystems, z.B. Windows, weist den schwerwiegenden Nachteil auf, dass zum Nutzerwechsel der Zugriff auf sämtliche Patientendaten beendet werden, alle Anwendungen gestoppt und das Betriebssystem heruntergefahren und wieder hochgefahren werden muss. Diese Abläufe sind äußerst zeitaufwändig.
- 25 Darüber hinaus steht dem nächsten Nutzer nicht der aktuelle Stand der Benutzeroberfläche und der darin enthaltenen Patientendaten zur Verfügung, falls diese als temporäre Informationen beim Herunterfahren des Betriebssystems verloren gehen.
- 30
- Als Abhilfe wird bei der Authentifizierung auf Betriebssystem-Ebene daher bislang mit sogenannten Gruppen-Accounts gearbeitet, die durch Gruppen von Nutzern verwendet werden, die
- 35 sämtlich die gleichen Zugriffsrechte erhalten sollen. Die Authentifizierung von Nutzern im Rahmen von Gruppen-Accounts

3

bringt jedoch den Nachteil mit sich, dass weder durch die Datenverarbeitungseinrichtung noch durch die darauf laufenden Anwendungs-Programme feststellbar ist, welcher Nutzer jeweils aktuell arbeitet. Da dies die Protokollierung der Datenutzeraktionen unmöglich machen würde, erfolgen Nutzerwechsel bei Benutzung von Gruppen-Accounts dadurch, dass die laufende Anwendung beendet und durch den neuen Nutzer neu gestartet werden muss. Temporäre Daten der laufenden Anwendung gehen zwar auch beim Beenden der Anwendung statt des Betriebssystems verloren, der Zeitverlust ist jedoch gegenüber dem Neustart des Betriebssystems geringer.

Der unter Aspekten ökonomischer Arbeitsweise nicht vertretbare Zeitverlust führt bislang häufig dazu, dass Nutzer an bildgebenden medizinischen Datenverarbeitungseinrichtungen nicht authentifiziert werden. Stattdessen erfolgen Identifikation und Autorisierung von Nutzern durch die rein physische Kontrolle des Zugriffs auf die bildgebende Einrichtung, d.h. durch eine simple Zugangskontrolle zu dem Raum in dem die Einrichtung steht. Insbesondere die Protokollierung von Datenzugriffen durch Nutzer ist an einer solchen Einrichtung nur indirekt möglich, in dem z.B. abgeglichen wird, welcher Nutzer zum Zeitpunkt eines Datenzugriffs in dem Raum der Einrichtung zugegen war. Diese Art der Protokollierung ist aufwändig und langfristig nicht im Nachhinein rekonstruierbar.

Die beschriebenen Nachteile treten vor allem in medizinischen Arbeitsumgebungen auf, wo bereits grundsätzlich unter großem Zeitdruck gearbeitet wird, der sich in Notfallsituationen noch wesentlich verschärfen kann. Sie wirken sich jedoch auch auf andere Datenverarbeitungseinrichtungen aus, die mit sensiblen Daten arbeiten, z.B. im Finanzwesen, in Forschung und Entwicklung, im Versicherungswesen oder bei der Bearbeitung demografischer Fragen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren zum schnellen Anmelden von Nutzern an Datenverarbeitungseinrich-

tungen anzugeben, an denen sensible Daten verarbeitet werden und an denen daher die Authentifizierung des Nutzers erforderlich ist. Unter sensiblen Daten sollen dabei insbesondere personenbezogene Angaben zum gesundheitlichen oder finanziellen Status oder in sonstigem Bezug zu Persönlichkeitsrechten verstanden werden.

Die Erfindung löst diese Aufgabe durch ein Verfahren mit den Verfahrensschritten des ersten Patentanspruchs.

Ein Grundgedanke der Erfindung besteht darin, die Anmeldung von Nutzern an Datenverarbeitungseinrichtungen durch eine Authentifizierungs-Instanz erfolgen zu lassen, die unabhängig vom Login an einem Betriebssystem oder einer laufenden Anwendung arbeitet. Unabhängig soll dabei so verstanden werden, dass die Anmeldung eines Nutzers nicht den Neustart des Betriebssystems oder der Anwendung erforderlich macht. Unter Authentifizierung sollen dabei die Identifikation einer Person und die Zuerkennung von Zugriffsrechten für Daten, Software und Hardware für diese Person verstanden werden. Die Authentifizierungs-Instanz ermöglicht den Wechsel des Nutzers, also eine Neu-Authentifizierung, bei laufendem Betriebssystem und laufender Anwendung oder Anwendungen.

Dadurch kann ein Nutzerwechsel zum einen schnell durchgeführt werden, da der Zeitaufwand für das Beenden und Neustarten von Anwendung oder Betriebssystem eingespart wird. Zum anderen kann ein neuer Nutzer nach Nutzerwechsel sämtlichen temporären Daten, wie aktuell bearbeitete Patientendaten oder die aktuelle Konstellation der Anwendung oder Anwendungen weiter benutzen, da sie nicht durch einen Neustart verloren gehen. Weiter ist der Nutzerwechsel ausreichend schnell, um insbesondere an Datenverarbeitungseinrichtungen eingesetzt werden zu können, an denen unter enormem Zeitdruck gearbeitet werden muss. Dadurch kann auch an solchen Einrichtungen eine ständig aktuelle Nutzer-Identität ermittelt werden, die z.B. zur

vollständigen Protokollierung aller Zugriffe genutzt werden kann.

5 In einer vorteilhaften Ausgestaltung der Erfindung ermöglicht die Authentifizierungs-Instanz den Nutzerwechsel unter Beibe-
haltung aller temporären Daten, wie aktuell bearbeiteten Pa-
tientendaten, aktuellen Anwendungseinstellungen oder Sichten,
10 in Abhängigkeit von einer Eingabe eines Nutzers, der dies wünscht. Es wird also Daten und der gesamte Anwendungs-
Kontext erhalten. Durch die Beibehaltung des aktuellen Status
können verschiedene Nutzer an der gleichen Datenverarbei-
tungseinrichtung die gleichen Daten in gleichbleibendem An-
wendungs-Kontext in schnellem Wechsel bearbeiten. Gleichzei-
15 derzeit gewährleistet, dass die abwechselnden Nutzer jeweils ausreichende Zugriffsrechte besitzen, um mit den gleichen Da-
ten arbeiten zu dürfen.

20 In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden sämtliche Nutzeraktionen unter Angabe von Informatio-
nen zu deren Identität protokolliert. Die für die Protokol-
lierung zu verwendende Identität wird dabei durch die Authen-
tizierungs-Instanz vorgegeben, die jeweils Identität und
25 Autorisierung gleichzeitig ermittelt. Dadurch kann gewähr-
leistet werden, dass sämtliche Datenzugriffe unter Angabe ak-
tueller Nutzer-Identitäten der Protokollierung zugeführt wer-
den, da durch die Authentifizierungs-Instanz Datenzugriffe
ohne Vorliegen einer Nutzer-Identität nicht autorisiert wer-
den.

30 In einer weiteren vorteilhaften Ausgestaltung ermöglicht die Authentifizierungs-Instanz den Nutzerwechsel mit gleichzeiti-
ger Löschung des aktuellen Status der bearbeiteten Daten und
der Benutzeroberfläche, d.h. der aktuellen Bildschirm-
35 Ansichten. Die Löschung erstreckt sich dabei ausschließlich auf temporäre Daten während dauerhaft gespeicherte Daten er-
halten bleiben. Der Nutzerwechsel mit Löschung des aktuellen

Status erfolgt auf eine entsprechende Eingabe des aktuellen Nutzers hin. Er ermöglicht es dem Nutzer, sich von der Bearbeitung von Daten sowie von der laufenden Anwendung abzumelden, ohne dass dafür die Anwendung oder gar das Betriebssystem beendet werden müssten.

- Dadurch kann ein Nutzer seine Arbeit an der Datenverarbeitungseinrichtung beenden ohne dass der nachfolgende Nutzer die Anwendung oder gar das Betriebssystem neu starten müsste. Dies erspart dem nachfolgenden Nutzer den mit einem Neustart verbundenen Zeitaufwand, da er nach seiner Authentifizierung an der Einrichtung unmittelbar in der laufenden Anwendung weiterarbeiten kann.
- In einer weiteren vorteilhaften Ausgestaltung der Erfindung wird der Nutzerwechsel bei Eintreten einer bestimmten Bedingung, z.B. nach Zeitablauf, analog zu einem Bildschirmschoner automatisch initiiert. Dabei werden ebenso wie bei einem Bildschirmschoner die aktuell dargestellten Anwendungsdaten temporär gelöscht, also unkenntlich gemacht aber in der Einrichtung beibehalten. Durch Ausführen einer Aktion an der Datenverarbeitungseinrichtung bei aktivierter Bildschirmschoner-Instanz, z.B. Tastendruck oder Mausbewegung, wird eine Abfrage zur aktuellen Authentifizierung des Nutzers ausgelöst. Wird durch die Authentifizierung festgestellt, dass der Nutzer nicht gewechselt hat, wird der vorige Status der Darstellung und der temporären Datenstände wieder hergestellt und die Arbeit kann fortgesetzt werden. Wird in Abweichung davon festgestellt, dass ein anderer Nutzer mit geringeren Zugriffsrechten an der Einrichtung arbeiten will, wird der vorherige Darstellungsstatus und temporäre Datenstand gelöscht oder in seinem Inhalt um die nicht zugriffsberechtigten Teile reduziert. Temporären Anwendungsdaten gehen bei der Reduzierung verloren. Wird statt dessen festgestellt, dass der neue Nutzer weitergehende Zugriffsrechte besitzt, so kann je nach vorgebbaren Einstellungen entweder der vorherige An-

zeigestatus und Datenstand wieder hergestellt oder ebenfalls inhaltlich reduziert werden.

Die Funktionalität in Anlehnung an einen Bildschirmschoner erhöht die Sicherheit der Einrichtung im Umgang mit sensiblen Daten, da die Einrichtung z.B. in Fällen, in denen der Nutzer die Arbeit plötzlich und ohne vorherige Abmeldung beenden muss, Zugriffe automatisch sperrt und eine Neu-Authentifizierung verlangt.

10

In einer weiteren vorteilhaften Ausgestaltung der Erfindung veranlasst die Authentifizierungs-Instanz bei fehlerhaften Eingaben zur Identität oder Passwort eines Nutzers automatisch eine Sperrung der Einrichtung auf Betriebssystem-Ebene, z.B. durch Herunterfahren des Betriebssystems. Dadurch wird die Sicherheit im Umgang mit den durch die Einrichtung verarbeiteten sensiblen Daten erhöht, da Fehleingaben durch nicht berechnigte Personen automatisch zu einem Zustand der Einrichtung führen, das maximalen Zugriffsschutz bietet. Insbesondere werden so Möglichkeiten zur Manipulation der Authentifizierungs-Instanz durch Schwachstellen, die vom Betriebssystem aus angreifbar wären, ausgeschlossen. Die Sperrung von Datenzugriffen auf Ebene des Betriebssystems bildet die höchste Barriere gegenüber Manipulationsversuchen.

25

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren näher erläutert. Es zeigen:

- FIG 1 Systemarchitektur mit Authentifizierungs-Instanz,
FIG 2 Authentifizierungs-Verfahren als Flussdiagramm.

In FIG 1 ist eine Systemarchitektur zur Ausführung des erfindenen Verfahrens schematisch dargestellt. Die Darstellung gibt lediglich die funktionalen Instanzen der Architektur wieder, ohne direkten Bezug auf einrichtungsmäßige Repräsentationen dieser Instanzen, z.B. durch bestimmte Hardware-Komponenten, zu nehmen.

35

Dargestellt ist ein erstes Anwendungs-Programm 71 und ein zweites Anwendungs-Programm 73 zur Verarbeitung sensibler Daten. Bei den sensiblen Daten kann es sich z.B. um medizinische Befunddaten, diagnostische Bilddaten, Informationen zu Finanzen oder zu Versicherungen oder demographische Daten handeln. Die Daten sollen dadurch als sensibel charakterisiert sein, dass sie, wenigstens teilweise, geheimhaltungsbedürftig sind und nur berechtigten Nutzern zugänglich sein sollen.

Die Anwendungs-Programme 71,73 können z.B. Bildgebungsprogramme in der medizinischen Diagnostik, Betrachtungsprogramme für elektronische Patientendaten, Programme für finanzielle Transaktionen, statistische Auswertungen oder Buchhaltung sein. Durch die Anwendungs-Programme 71,73 kann ein Nutzer Daten einsehen, verändern, erzeugen oder löschen. Im Rahmen der Bearbeitung von Daten können außerdem andere Anwendungs-Programme gestartet oder die Anwendungs-Programme 71,73 beendet werden. Es spielt dabei keine Rolle, ob nur ein oder mehrere Anwendungs-Programme 71, 73 gestartet werden. Wesentlich ist lediglich, dass sie über eine gemeinsame Schnittstelle, wie sie in ähnlicher Weise von Bildschirmschoner-Schnittstellen bekannt ist, mit der unten beschriebenen Authentifizierungs-Instanz 75 kommunizieren können.

Die Anwendungs-Programme 71,73 sind durch eine Authentifizierungs-Instanz 75 abgesichert, die sämtliche Zugriffe kontrolliert. Die Authentifizierungs-Instanz 75 stellt die Identität des Nutzers fest, indem entweder die Eingabe eines Nutzernamens und eines Passworts gefordert wird, oder indem auf eine biometrische Messeinrichtung, z.B. zur Ermittlung des Fingerabdrucks oder der Irisgestalt oder auf einen Chip oder Transponder, Lesgerät zugegriffen wird.

In Abhängigkeit von der ermittelten Identität ordnet die Authentifizierungsinstanz 75 dem Nutzer Zugriffsrechte für Da-

- ten, Software und Hardware zu. Sie kann dabei über alle Zugriffsrechte, die das Betriebssystem 79 ihr gewährt, verfügen; das Betriebssystem 79 gibt als den maximal möglichen Umfang an Zugriffsrechten vor. Dies schließt den Zugriff auf
- 5 Daten 87, Hardware 85 und Software 71,73 ein, so dass die Authentifizierungs-Instanz 75 die Benutzung aller Einrichtungs-Ressourcen einschließlich der Anwendungs-Programme 71,73 freigeben oder Sperren kann.
- 10 Insofern arbeitet die Authentifizierungs-Instanz 75 zwar in dem vom Betriebssystem 79 vorgegebenen Rahmen und nur dann, wenn auch das Betriebssystem 79 gestartet wurde. Innerhalb des vorgegebenen Rahmens arbeitet sie jedoch unabhängig vom Betriebssystem 79 und insbesondere unabhängig von einem Neu-
- 15 Start des Betriebssystems 79. Zugriffe durch den Nutzer erfolgen ausschließlich über die Benutzeroberfläche 81, die durch die Authentifizierungs-Instanz 75 kontrolliert wird.
- Die Authentifizierungs-Instanz 75 weist zwei Unterinstanzen
- 20 auf, eine Bildschirmschoner-Instanz 76 und eine Instanz zum Nutzerwechsel 77. Die Bildschirmschoner-Instanz 76 sorgt ähnlich bekannten Bildschirmschonern dafür, dass die Benutzeroberfläche 81 bei Eintreten bestimmter Bedingungen, z.B. nach Zeitablauf, gelöscht wird. Mit gelöscht ist gemeint, dass die
- 25 bildliche Darstellung der Benutzeroberfläche 81 auf einem Anzeigegerät, z.B. einem Bildschirm, so verändert wird, dass keine geheimhaltungsbedürftigen Daten mehr angezeigt werden, sie wird also inhaltlich reduziert bzw. neutralisiert. Damit soll verhindert werden, dass nach eiligem Verlassen der Einrichtung ohne ordnungsgemäße Abmeldung durch den vorhergehenden Nutzer sensible Daten unkontrolliert einsehbar bleiben.
- 30 Die Bildschirmschoner-Instanz 76 kann in Analogie zu bekannten Bildschirmschonern dadurch aktiviert werden, dass eine
- 35 bestimmte Zeit ohne jedwede Nutzereingabe an der Einrichtung verstrichen ist. Zur Erhöhung der Datensicherheit kann jedoch

10

auch vorgesehen sein, dass die Bildschirmschoner-Instanz 76 unabhängig von Nutzereingaben aktiviert wird.

Um die Bildschirmschoner-Instanz 76 zu deaktivieren und zur ursprünglichen Benutzeroberfläche 81 zurückzugelangen, muss sich der Nutzer erneut, wie oben beschrieben, identifizieren lassen. Die Darstellung der Benutzeroberfläche 81 nach der Deaktivierung hängt davon ab, ob der Nutzer inzwischen gewechselt hat und ggf. welchen Umfang die Rechte eines neuen Nutzers aufweisen. Sie kann je nachdem inhaltlich unverändert bleiben oder inhaltlich verändert sein.

Fand kein Nutzerwechsel statt und wurde lediglich der vorherige Nutzer erneut authentifiziert, so steht nach Deaktivierung der Bildschirmschoner-Instanz 76 die Benutzeroberfläche 81 in exakt dem Zustand wieder zur Verfügung, den sie vor Aktivierung der Bildschirmschoner-Instanz 76 hatte, der gesamte Anwendungs-Kontext bleibt also erhalten. Dies schließt den Status der laufenden Anwendungen, z.B. welche Fenster geöffnet sind und welche Anwendungs-Module geladen sind, ebenso wie die aktuell angezeigten sensiblen Daten ein und deren temporären Bearbeitungsstatus. Auch temporäre Änderungen der Daten, die noch nicht durch die Datenverarbeitungseinrichtung gespeichert wurde, stehen wie vorher zur Verfügung und können gespeichert oder zur weiteren Verarbeitung genutzt werden.

Hat jedoch ein Nutzerwechsel stattgefunden und stellt sich durch die Authentifizierung heraus, dass der neue Nutzer gegenüber dem vorhergehenden Nutzer eingeschränkte Zugriffsrechte hat, so wird die Benutzeroberfläche 81 je nach Umfang und Art der Einschränkung inhaltlich reduziert oder völlig neutral gemacht, der Anwendungs-Kontext bleibt also nur eingeschränkt erhalten. Hat der neue Nutzer z.B. keine Berechtigung, auf die zuvor angezeigten Daten zuzugreifen, so werden diese aus der Benutzeroberfläche 81 entfernt und sind auch durch die Anwendungs-Programme 71, 73 nicht mehr zugänglich. Hat der neue Nutzer z.B. nur Berechtigung zur Einsichtnahme

11

und nicht zur Veränderung von Daten, so werden evt. gesperrte Datenveränderungsmodule der Anwendungs-Programme 71,73 aus der Benutzeroberfläche 81 entfernt, oder reine Datenverarbeitungsanwendungen geschlossen.

5

Hat der neue Nutzer gegenüber dem vorhergehenden erweiterte Rechte, so kann je nach vorgebbarer Einstellung entweder der vorherige Anwendungs-Kontext, also Benutzeroberfläche 81 samt aktuellen Daten, vollständig wieder hergestellt werden oder ein beliebiger anderer Zustand, z.B. ein erweiterter Umfang an sensiblen Daten oder Funktionsmodulen der Anwendungs-Programme 71,73 verfügbar gemacht werden.

Die Nutzerwechsel-Instanz 77 wird zum einen in Abhängigkeit von der Aktivierung der Bildschirmschoner-Instanz 76 aktiv, zu dessen Deaktivierung eine erneute Authentifizierung des Nutzers erforderlich ist. Zum anderen kann die Nutzerwechsel-Instanz 76 auch durch den Nutzer aktiviert werden. Die Aktivierung erfolgt z.B. dann, wenn der Nutzer sich von der Einrichtung durch eine entsprechende Eingabe abmeldet. Auf die Abmeldung hin werden sämtliche aktuell angezeigten Daten aus der Benutzeroberfläche 81 und aus den Anwendungs-Programmen 71,73 entfernt, wobei sämtliche temporären Informationen wie vorläufige Änderungen der Daten oder der aktuelle Status der Anwendungs-Programme 71,73 ab sofort nicht mehr zur Verfügung stehen. Je nach vorgebbarer Einstellung können temporäre Daten entweder vollständig verworfen oder automatisch gespeichert werden. Die laufende Anwendungs-Programme 71,73 wird dadurch in einen neutralen Ausgangszustand zurückversetzt, in dem der folgende Nutzer seine Arbeit beginnen kann.

Durch eine entsprechende Eingabe des Nutzers kann die Nutzerwechselinstanz 77 jedoch auch veranlassen, dass der aktuelle Nutzer abgemeldet wird, jedoch sämtliche temporären Daten weiterhin auf der Benutzeroberfläche 81 zur Verfügung stehen. Diese Möglichkeit ist vor allem dann von Bedeutung, wenn der folgende Nutzer mit den aktuell angezeigten Daten im gegen-

12

wärtigen Status der Anwendungs-Programme 71,73 weiterarbeiten soll. Durch einen derartigen Wechsel des Nutzers bleibt die Autorisierung von Zugriffsrechten erhalten, während die Identität des Nutzers wechselt. Die jeweils aktuelle Nutzer-
5 Identität steht dann zur vollständigen Protokollierung aller laufenden Nutzeraktionen und Zugriffe zur Verfügung.

Stellt die Nutzerwechsel-Instanz 77 bei der Neu-Authentifizierung des Nutzers fest, dass dieser geringere Rechte besitzt als der vorhergehende Nutzer, so dass temporäre Daten auf der Benutzeroberfläche 81 nicht mehr dargestellt werden dürften und verloren gehen würden, so kann an den Nutzer eine entsprechende Warnmeldung ausgegeben werden, z.B. in einem entsprechenden Hinweis-Fenster auf der Benutzeroberfläche 81.
10 Dadurch besteht für den vorhergehenden Nutzer die Möglichkeit, durch eigene Anmeldung an der Einrichtung den vorherigen, temporären Status der Daten und Programm-Sichten wieder herzustellen und nötigenfalls in der Einrichtung zu speichern. Falls dies nicht gewünscht wird, so kann durch Bestätigung der Warnmeldung ein neuer Anwendungs-Status mit veränderter Benutzeroberfläche 81 und unter Inkaufnahme von Verlusten temporärer Daten erzeugt werden.
15 20

An der in FIG 1 gewählten zeichnerischen Darstellung wird
25 sichtbar, dass die Authentifizierungs-Instanz 75 samt Benutzeroberfläche 81 auf die Anwendungs-Programme 71,73 sowie das laufende Betriebssystem 79 aufsetzt. Dies ist für die Erfindung von großer Bedeutung, da die Zugriffskontrolle auf einer Ebene stattfindet, die oberhalb der Betriebssystem-Ebene 79 und der Anwendungs-Programm-Ebene 71,73 angesiedelt ist. Daher können Änderungen der Nutzer-Autorisierung und -Identifizierung vorgenommen werden, ohne dazu laufende Anwendungs-Programme 71,73 oder das Betriebssystem 79 neu starten zu müssen. Dies beschleunigt die Neu-Authentifizierung bei Nutzerwechsel erheblich.
30 35

13

Die Möglichkeit zum schnellen Nutzerwechsel macht das Verfahren an Arbeitsplätzen praktikabel, an denen unter großem Zeitdruck gearbeitet werden muss, z.B. in der Medizin oder Notfall-Medizin. Infolge dessen steht an solchen Arbeitsplätzen durch Verwendung des Verfahrens die Möglichkeit des laufenden, vollständigen Protokollierung aller Nutzeraktionen zur Verfügung. Eine derartige Protokollierung ist insbesondere durch den Datenschutz im Gesundheitswesen zwingend vorgeschrieben. Ein weiterer Vorteil besteht darin, dass Arbeitsplätze, die durch einen Bildschirmschoner geschützt werden, nicht mehr dadurch blockiert werden können, dass das Bildschirmschoner-Passwort des vorherigen Nutzers oder das generelle Bildschirmschoner-Passwort nicht bekannt ist. Statt dessen erfolgt die Deaktivierung der Bildschirmschoner-Instanz 76 durch eine Neu-Authentifizierung des Nutzers, der dadurch seine eigenen Identifikations-Daten eingeben muss.

In FIG 2 sind die Schritte des Verfahrens als Flussdiagramm dargestellt. In Schritt 1 erfolgt die Anmeldung am Betriebssystem, das in Schritt 3 in einer von der Anmeldung abhängigen Betriebssystem-Konfiguration arbeitet. Die Zugriffsrechte bei Anmeldungen am Betriebssystem sind so beschaffen, dass die Kontrolle aller Zugriffe durch die Authentifizierungs-Instanz 75 gewährleistet werden kann. Eine Anmeldung am Betriebssystem 79 mit umfassenden Datenzugriffsrechten bleibt dabei Systemadministratoren vorbehalten, während Anwendungsnutzer nur Zugriff über die Authentifizierungs-Instanz 75 erhalten.

In Schritt 5 wird das Anwendungs-Programm 71,73 gestartet. Da bereits die Nutzung des Anwendungs-Programms 71,73 der Einschränkung von Zugriffsrechten unterliegen kann, wird unmittelbar nach dem Starten des Anwendungs-Programms 71,73 oder der Anwendungs-Programme 71,73 in Schritt 7 die Eingabe eines Nutzer-Logins gefordert. Die Eingabe kann, wie oben beschrieben, durch manuelle Eingabe von Daten oder Messungen biometrischer oder sonstiger Informationen erfolgen. Sie kann zum

Zusammenfassung

Verfahren zum Anmelden von Nutzern an Datenverarbeitungseinrichtungen

5

Die Erfindung betrifft ein Verfahren zum Anmelden eines Nutzers an einer Datenverarbeitungseinrichtung mit einem Betriebssystem (79) und einem Datenverarbeitungs-Programm (71, 73). In einem ersten Schritt (7, 9) werden Daten zur Authentifizierung des Nutzers ermittelt, in einem zweiten Schritt (13) in Abhängigkeit von den Authentifizierungs-Daten eine Identität und ein Zugriffsrecht festgelegt, und in einem dritten Schritt (29) in Abhängigkeit von dem festgelegten Zugriffsrecht der Zugriff auf das Datenverarbeitungs-Programm (71, 73) und/oder auf sensible Daten (85) freigegeben. Gemäß der Erfindung sind die Schritte unabhängig von einem Starten des Betriebssystems (79) oder der Datenverarbeitungsanwendung (71, 73). In einer besonders vorteilhaften Ausgestaltung der Erfindung kann ein Nutzerwechsel durch Abmelden des Nutzers und Anmelden eines neuen Nutzers stattfinden, bei dem der Anwendungskontext, also Benutzeroberfläche (81) und aktuell bearbeitete Daten (85) erhalten bleibt.

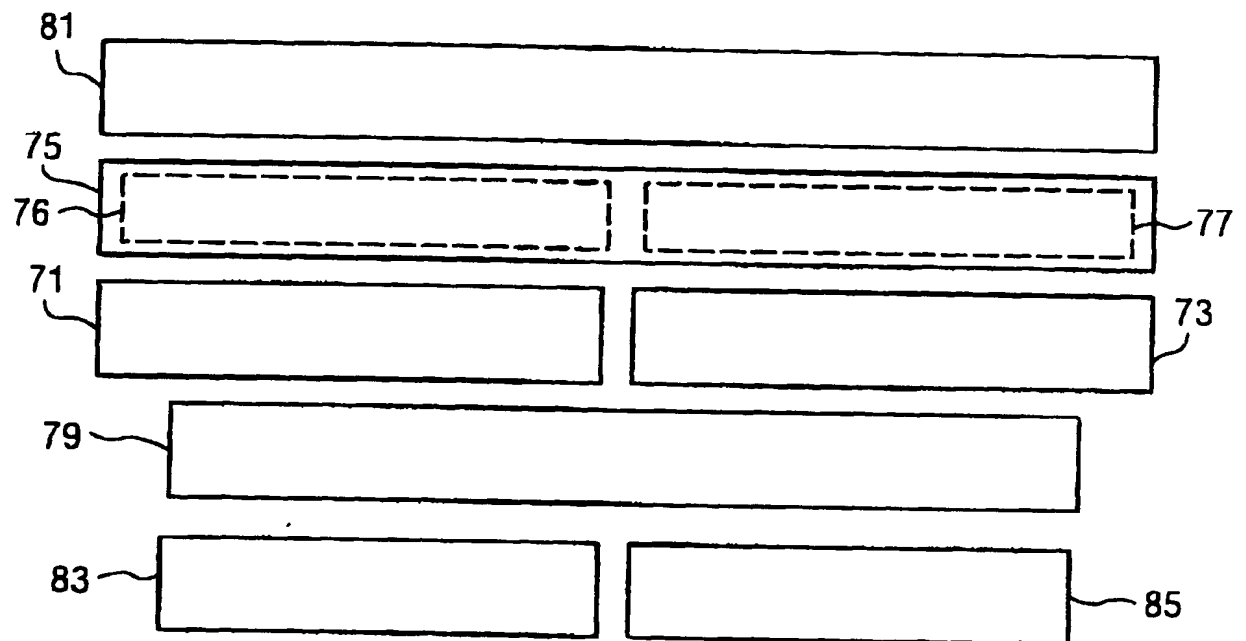
10

15

20

FIG 1

FIG 1



United States Patent & Trademark Office

Office of Initial Patent Examination

Application papers not suitable for publication

SN 60430206

Mail Date 12/01/02

- ☒ Non-English Specification
- ☐ Specification contains drawing(s) on page(s) _____ or table(s) _____
- ☐ Landscape orientation of text ☐ Specification ☐ Claims ☐ Abstract
- ☐ Handwritten ☐ Specification ☐ Claims ☐ Abstract
- ☐ More than one column ☐ Specification ☐ Claims ☐ Abstract
- ☐ Improper line spacing ☐ Specification ☐ Claims ☐ Abstract
- ☐ Claims not on separate page(s)
- ☐ Abstract not on separate page(s)
- ☐ Improper paper size -- Must be either A4 (21 cm x 29.7 cm) or 8-1/2"x 11"
- ☐ Specification page(s) _____ ☐ Abstract
- ☐ Drawing page(s) _____ ☐ Claim(s)
- ☐ Improper margins
- ☐ Specification page(s) _____ ☐ Abstract
- ☐ Drawing page(s) _____ ☐ Claim(s)
- ☐ Not reproducible
- | <u>Reason</u> | <u>Section</u> |
|---|--|
| <input type="checkbox"/> Paper too thin | <input type="checkbox"/> Specification page(s) _____ |
| <input type="checkbox"/> Glossy pages | <input type="checkbox"/> Drawing page(s) _____ |
| <input type="checkbox"/> Non-white background | <input type="checkbox"/> Abstract |
| | <input type="checkbox"/> Claim(s) |
- ☐ Drawing objection(s)
- ☐ Missing lead lines, drawing(s) _____
- ☐ Line quality is too light, drawing(s) _____
- ☐ More than 1 drawing and not numbered correctly
- ☐ Non-English text, drawing(s) _____
- ☐ Excessive text, drawing(s) _____
- ☐ Photographs capable of illustration, drawing(s) _____

